**Chapter 3**

**Literature SURWAY**

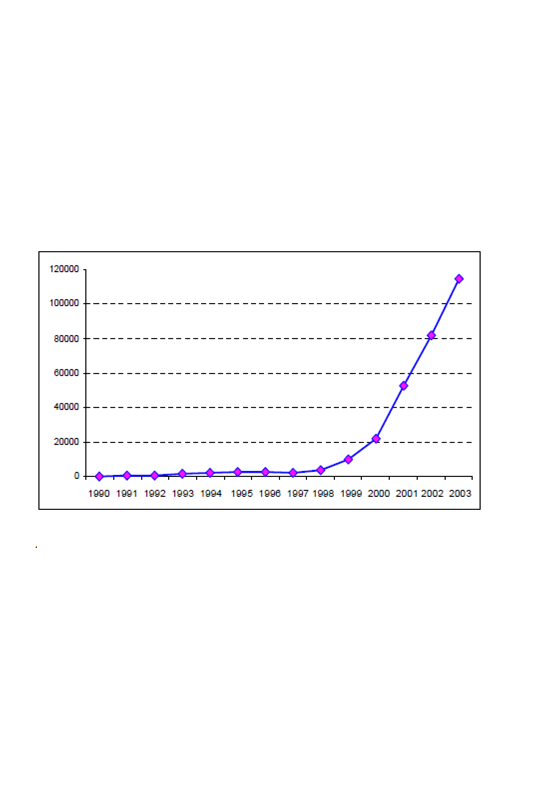
**3.1 Background Study**

There are a number of common attacks on networked computers which, for their detection, require information from multiple sources, one of the most common of these is the so called doorknob attack. In a doorknob attack the goal is to discover, and gain access to, insufficiently protected systems. The incidents, which have raised the most concern in recent years, are the Denial-of-Service (DOS) attacks whose sole purpose is to reduce or eliminate the availability of a service provided over the Internet, to its legitimate users. The first kind of attacks can be avoided by patching-up vulnerable software and updating the host systems from time to time. In comparison, the second kinds of DOS attacks are much more difficult to defend. This works by sending a large number of packets to the target, so that some critical resources of the victim are exhausted and the victim can no longer communicate with other users. For second type of attack in IDS is most popular tool.

Packets sent using the IP protocol include the IP address of the sending host. The recipient directs replies to the sender using this source address. However, the correctness of this address is not verified by the protocol. The IP protocol specifies no method for validating the authenticity of the packet’s source. This implies that an attacker could forge the source address to be any he desires. This is a well-known problem and has been well described in all but a few rare cases; sending Network packets are done for illegitimate purposes. The original path identification marking is based on the use of the packet’s TTL field as an index into the IP Identification field where a router should add its marks. This method is not as lightweight as the Stack Path identification method. Legacy routers have a harmful affect on the original Path identification scheme because they decrement the TTL of a packet but do not add any markings. The Stack Path identification scheme is robust to legacy routers and even includes the write-ahead scheme to incorporate markings for single legacy routers in the path.

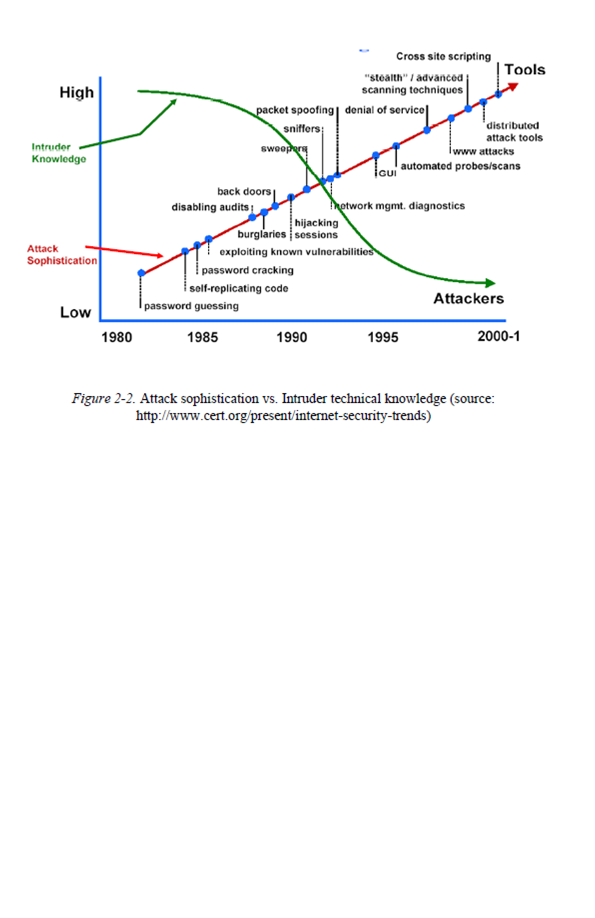
**3.2 Related Work**

Aleksandar Lazarevic, Vipin Kumar, Jaideep Srivastava provide an overview of the state of the art in intrusion detection research. Intrusion detection systems are software and/or hardware components that monitor computer systems and analyze events occurring in them for signs of intrusions. Due to widespread diversity and complexity of computer infrastructures, it is difficult to provide a completely secure computer system. Therefore, there are numerous security systems and intrusion detection systems that address different aspects of computer security. They first proposed taxonomy of computer intrusions, along with brief descriptions of major computer attack categories. Second, a common architecture of intrusion detection systems and their basic characteristics are presented. Third, taxonomy of intrusion detection systems based on five criteria (information source, analysis strategy, time aspects, architecture, response) is given. Finally, intrusion detection systems are classified according to each of these categories and the most representative research prototypes are briefly described.

As reported by theComputer Emergency Response Team/Coordination Center (CERT/CC)[08], the number of computer attacks has increased exponentially in the pastfew years (Figure 2-1). In addition, the severity and sophistication of theattacks is also growing (Figure 2-2). For example, Slammer/Sapphire Wormwas the fastest computer worm in history. As it began spreading throughoutthe Internet, it doubled in size every 8.5 seconds and infected at least 75,000hosts causing network outages and unforeseen consequences such ascancelled airline flights, interference with elections, and ATM failures [04].Earlier, the intruders needed profound understanding of computers andnetworks to launch attacks. However, today almost anyone can exploit thevulnerabilities in a computer system due to the wide availability of attacktools (Figure 2-2).

**Figure 2-1.Growth rate of cyber incidents reported to Computer Emergency Response Team/Coordination Center (CERT/CC)**

The conventional approach for securing computer systems is to designsecurity mechanisms, such as firewalls, authentication mechanisms, VirtualPrivate Networks (VPN), that create a protective “*shield*” around them.However, such security mechanisms almost always have inevitablevulnerabilities and they are usually not sufficient to ensure complete securityof the infrastructure and to ward off attacks that are continually being adapted to exploit the system’s weaknesses often caused by careless designand implementation flaws. This has created the need for security technologythat can monitor systems and identify computer attacks. This component iscalled intrusion detection and is a complementary to conventional securitymechanisms.

****

**Fig. 2.2 Attack sophistication vs. Intruder technical knowledge**

The National Institute of Standards and Technology classifies intrusiondetection as “*the process of monitoring the events occurring in a**computer system or network and analyzing them for signs of intrusions,**defined as attempts to compromise the confidentiality, integrity, availability,**or to bypass the security mechanisms of a computer or network*"[04].Intrusions in computer systems are usually caused by attackers accessingthe systems from the Internet, or by authorized users of the systems whoattempt to misuse the privileges given to them and/or to gain additionalprivileges for which they are not authorized. An Intrusion Detection System(IDS) can be defined as a combination of software and/or hardwarecomponents that monitors computer systems and raises an alarm when anintrusion happens.This chapter provides an overview of the current status of research inintrusion detection. It first provides an overview of different types ofcomputer intrusions, and then introduces a more detailed taxonomy ofintrusion detection systems with an overview of important research in thefield. Both taxonomies are illustrated and supported with several well knownexamples of computer attacks and intrusion detection techniques. Several surveys in the intrusion detection have been published in the past [04]. However, the growth of the field has been very rapid, and many new ideas have since emerged. The survey in this chapter attempts to build upon these earlier surveys, but is more focused on intrusion detection projects proposed in academic institutions and researchorganizations than on commercial intrusion detection systems, primarily dueto the lack of detailed technical information available on commercialproducts. The reader interested in commercial IDSs is referred to a survey ofIDS products and to web sites that maintain lists of such systems [04].